Exhibit A

Click here to Respond to Selected Documents

Sort Date Entries: Descending Ascending

Display Options: All Entries

05/22/2025

Corporation Served
Document ID - 25-SMCC-8212; Served To - AMERICAN MULTISPECIALTY GROUP, INC.,; Served Date - 05/20/2025; Served Time - 13:52:00; Service Type - SP; Reason Description - SERV; Service Text -

Notice of Service
Return of Service of Summons.
Filed By: JOHN FRANCIS GARVEY JR
On Behalf Of: MARTHA PROFFITT

05/19/2025

Summons Issued-Circuit
Document ID: 25-SMCC-8212, for AMERICAN MULTISPECIALTY GROUP, INC. Summons Attached in PDF Form for Attorney to Retrieve from Secure Case.Net and Process for Service.

Motion Special Process Server
Request for Appointment of Special Process Server.
Filed By: JOHN FRANCIS GARVEY JR
On Behalf Of: MARTHA PROFFITT

Memorandum Filed
Memorandum to the Clerk.
Filed By: JOHN FRANCIS GARVEY JR
On Behalf Of: MARTHA PROFFITT

Notice of Dismissal
NO SUMMONS ISSUED DUE TO THE PETITION MISSING THE DEFENDANT'S SERVICE ADDRESS. E-FILE A MEMO INCLUDING THE DEFENDANT'S SERVICE ADDRESS SO THE CASE CAN BE FURTHER PROCESSED. FOR FUTURE REFERENCE, THE DFT'S SERVICE ADDRESS MUST BE LISTED ON THE PETITION UNDER THE DFT'S NAME. ONCE THE CORRECTION IS E-FILED, CONTACT THE CLERK AT 314-615-8470.

05/14/2025

Motion Special Process Server
Motion for Special Process Server.
Filed By: JOHN FRANCIS GARVEY JR
On Behalf Of: MARTHA PROFFITT

Filing Info Sheet eFiling

Filed By: JOHN FRANCIS GARVEY JR

Pet Filed in Circuit Ct
Class Action Petition.
Filed By: JOHN FRANCIS GARVEY JR

Judge Assigned
DIV 9

IN THE CIRCUIT COURT OF ST. LOUIS COUNTY
STATE OF MISSOURI

MARTHA PROFFITT, individually and on behalf of all others similarly situated, Plaintiff, v. AMERICAN MULTISPECIALTY GROUP, INC. d/b/a ESSE HEALTH, Defendant.	**Case No.:** **Division No.** **JURY TRIAL DEMANDED**

CLASS ACTION PETITION

COMES NOW Plaintiff Martha Proffitt ("Plaintiff"), individually and on behalf of all others similarly situated, by and through her undersigned counsel, brings this Class Action Complaint against American Multispecialty Group, Inc. d/b/a Esse Health ("Esse Health" or 'Defendant"). Plaintiff alleges the following upon information and belief based on and the investigation of counsel, except as to those allegations that specifically pertain to Plaintiff, which are alleged upon personal knowledge.

INTRODUCTION

1. Plaintiff and the proposed Class Members bring this class action lawsuit on behalf of all persons who entrusted Defendant with sensitive Personally Identifiable Information ("PII")[1] and Protected Health Information ("PHI") (collectively, "Private Information") that was impacted in a data breach that occurred in late April 2025 (the "Data Breach" or the "Breach").

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual.

2. Plaintiff's claims arise from Defendant's failure to properly secure and safeguard Private Information that was entrusted to it, and its accompanying responsibility to store and transfer that information.

3. Defendant is an independent physician group healthcare provider with 50 locations in the Greater St. Louis area in Missouri.[2]

4. Defendant had numerous statutory, regulatory, contractual, and common law duties and obligations, including those based on its affirmative representations to Plaintiff and Class Members, to keep their Private Information confidential, safe, secure, and protected from unauthorized disclosure or access.

5. In late April 2025, Defendant detected unusual activity on its IT Network.[3] The Data Breach caused Defendant's network systems to be taken offline.[4] In response to the incident, Defendant launched an investigation to determine the nature and scope of the Data Breach.[5]

6. Defendant admits that information in its system was accessed by an unauthorized actor, though it has provided little information regarding how the Data Breach occurred.[6]

7. Defendant failed to take precautions designed to keep individuals' Private Information secure.

8. Defendant owed Plaintiff and Class Members a duty to take all reasonable and necessary measures to keep the Private Information collected safe and secure from unauthorized access. Defendant solicited, collected, used, and derived a benefit from the Private Information, yet breached its duty by failing to implement or maintain adequate security practices.

---

[2] *About Us*, American Multispecialty Group, Inc. d/b/a Esse Health https://www.essehealth.com/about-us/ (last visited May 14, 2025).
[3] https://www.hipaajournal.com/esse-health-cyberattack/ (last visited May 14, 2025).
[4] *Id.*
[5] *Id.*
[6] *Id.*

9. The sensitive nature of the data maintained by Defendant and potentially compromised in the Data Breach, signifies that Plaintiff and Class Members have suffered irreparable harm. Plaintiff and Class Members have lost the ability to control their Private Information and are subject to an increased risk of identity theft.

10. Defendant, despite having the financial wherewithal and personnel necessary to prevent the Data Breach, nevertheless failed to use reasonable security procedures and practice appropriate to the nature of the sensitive, unencrypted information it maintained for Plaintiff and Class Members, causing the exposure of Plaintiff's and Class Members' Private Information.

11. As a result of Defendant's inadequate digital security and notice process, Plaintiff's and Class Members' Private Information was exposed to criminals. Plaintiff and the Class Members have suffered and will continue to suffer injuries including: financial losses caused by misuse of their Private Information; the loss or diminished value of their Private Information as a result of the Data Breach; lost time associated with detecting and preventing identity theft; and theft of personal and financial information.

12. Moreover, as an ongoing harm resulting from the Data Breach, Plaintiff and Class Members experienced disruptions in services because Defendant's IT Network went offline. These disruptions included delays in obtaining treatment, cancellation of medical appointments with providers, and inability to schedule medical appointments.

13. Plaintiff brings this action on behalf of all persons whose Private Information was compromised as a result of Defendant's failure to: (i) adequately protect the Private Information of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of Defendant's inadequate information security practices; (iii) effectively secure hardware containing protected Private Information using reasonable and adequate security procedures free of vulnerabilities and

incidents; and (iv) timely notify Plaintiff and Class Members of the Data Breach. Defendant's conduct amounts to at least negligence and violates federal and state statutes.

14. Plaintiff brings this action against Defendant for: negligence, negligence *per se*, unjust enrichment, breach of implied contract, breach of confidence, and violation of the Missouri Merchandise Practices Act, Mo. Rev. Stat. §§ 407.010, *et seq.*

15. Plaintiff seeks to remedy these harms and prevent any future data compromise on behalf of herself and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach and who remain at risk due to Defendant's inadequate data security practices.

PARTIES

Plaintiff

16. Plaintiff Martha Proffitt is a citizen and resident of Arnold, Missouri.

Defendant

17. Defendant is a corporation organized under the laws of the State of Missouri with its principal place of business located at 12655 Olive Boulevard, Floor 4, Saint Louis, Missouri, 63141.

JURISDICTION AND VENUE

18. The Court has jurisdiction over the parties because Defendant is a Missouri based corporation that can be found and served in the State of Missouri and regularly conducts business in the State.

19. Venue is proper because Defendant has its principal place of business within the State in St. Louis County.

FACTUAL ALLEGATIONS

A. Background on Defendant

20. Defendant is an independent physician group healthcare provider with 50 locations in the Greater St. Louis area in Missouri

21. Upon information and belief, Defendant made promises and representations to individuals, including Plaintiff and Class Members, that the Private Information collected from them would be kept safe and confidential, and that the privacy of that information would be maintained.[7]

22. Plaintiff and Class Members provided their Private Information to Defendant with the reasonable expectation and on the mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

23. As a result of collecting and storing the Private Information of Plaintiff and Class Members for its own financial benefit, Defendant had a continuous duty to adopt and employ reasonable measures to protect Plaintiff's and the Class Members' Private Information from disclosure to third parties.

B. The Data Breach

24. In late April 2025, Defendant detected unusual activity on its IT Network.[8] The Data Breach caused Defendant's network systems to be taken offline.[9]

25. In response to the incident, Defendant launched an investigation to determine the nature and scope of the Data Breach.[10]

---

[7] *Privacy Policy*, American Multispecialty Group, Inc. d/b/a Esse Health https://www.essehealth.com/privacy-policy/ (last visited May 14, 2025).
[8] https://www.hipaajournal.com/esse-health-cyberattack/ (last visited May 14, 2025).
[9] *Id.*
[10] *Id.*

26. As a result of the Data Breach, numerous patients reported that their healthcare was placed on hold, with medical appointments and scheduling delays occurring.[11]

27. Defendant admits that information in its system was accessed by an unauthorized actor, though it has provided little information regarding how the Data Breach occurred.[12]

28. Plaintiff's claims arise from Defendant's failure to safeguard Private Information provided by and belonging to its patients and failure to provide timely notice of the Data Breach.

29. Defendant failed to take precautions designed to keep its patients' Private Information secure.

30. While Defendant sought to minimize the damage caused by the Data Breach, it cannot and has not denied that there was unauthorized access to the sensitive Private Information of Plaintiff and Class Members.

31. Individuals affected by the Data Breach are, and remain, at risk that their data will be sold or listed on the dark web and, ultimately, illegally used in the future.

C. Defendant's Failure to Prevent, Identify, and Timely Report the Data Breach

32. Defendant admits that an unauthorized third party accessed its IT Network. Defendant failed to take adequate measures to protect its computer systems against unauthorized access.

33. The Private Information that Defendant allowed to be exposed in the Data Breach is the type of private information that Defendant knew or should have known would be the target of cyberattacks.

[11] https://healthexec.com/topics/health-it/cybersecurity/independent-provider-group-hit-cyberattack-delays-patient-care (last visited May 15, 2025).
[12] *Id.*

34. Defendant was not only aware of the importance of protecting the Private Information that it maintains, as alleged, it promoted its capability to do so, as evident from its Privacy Policy.[13]

35. Despite its own knowledge of the inherent risks of cyberattacks, and notwithstanding the FTC's data security principles and practices,[14] Defendant failed to disclose that its systems and security practices were inadequate to reasonably individuals' Private Information.

36. The FTC directs businesses to use an intrusion detection system to expose a breach as soon as it occurs, monitor activity for attempted hacks, and have an immediate response plan if a breach occurs.[15] Immediate notification of a Data Breach is critical so that those impacted can take measures to protect themselves.

37. Here, Defendant has yet to directly notify impacted individuals of the Data Breach.

D. Data Breaches Cause Disruptions That Put Patients at an Increased Risk of Harm

38. Cyber-attacks at medical facilities such as Defendant's are especially problematic because of the disruption they cause to the health treatment and overall daily lives of patients affected by the attack.

39. For instance, loss of access to patient histories, charts, images, and other information forces providers to limit or cancel patient treatment due to a disruption of service. This leads to a deterioration in the quality of overall care patients receive at facilities affected by cyber-attacks and related data breaches.

---

[13] *Privacy Policy*, American Multispecialty Group, Inc. d/b/a Esse Health https://www.essehealth.com/privacy-policy/ (last visited May 14, 2025).

[14] *Protecting Personal Information: A Guide for Business,* FED. TRADE COMM'N (Oct. 2016), https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business. (last visited May 14, 2025).

[15] *Id.*

40. Researchers have found medical facilities that experience a data security incident incur an increase in the death rate among patients' months and years after the attack.[16] Researchers have further found that at medical facilities that experience a data breach, the incident leads to a deterioration in patient outcomes, generally.[17]

41. Similarly, cyber-attacks and related data security incidents inconvenience patients; these inconveniences include, but are not limited, to the following:

a. rescheduling of medical treatment;

b. being forced to find alternative medical care and treatment;

c. delays or outright cancellation of medical care and treatment;

d. undergoing medical care and treatment without medical providers having access to a complete medical history and records; and

e. the indefinite loss of personal medical history.

E. <u>The Harm Caused by the Data Breach Now and Going Forward</u>

42. Victims of data breaches are susceptible to becoming victims of identity theft. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 17 C.F.R. § 248.201(9). When "identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance."[18]

---

[16] See Nsikan Akpan, *Ransomware and Data Breaches Linked to Uptick in Fatal Heart Attacks*, PBS (Oct. 24, 2019) https://www.pbs.org/newshour/science/ransomware-and-other-data-breaches-linked-to-uptick-in-fatal-heart-attacks (last visited May 13, 2025).

[17] See Sung J. Choi PhD., et al., *Data breach remediation efforts and their implications for hospital quality*, HEALTH SERVICES RESEARCH (Sept. 10, 2019) https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203 (last visited May 13, 2025).

[18] *Prevention and Preparedness*, New York State Police, https://troopers.ny.gov/prevention-and-preparedness (last visited May 14, 2025).

43. The types of data that may have been accessed and compromised here can be used to perpetrate fraud and identity theft.

44. Plaintiff and Class Members face a substantial risk of identity theft given that their Private Information was compromised in the Data Breach.

45. Stolen Private Information is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines. Law enforcement has difficulty policing the "dark web" due to this encryption, which allows users and criminals to conceal their identities and online activity.

46. When malicious actors infiltrate companies and copy and exfiltrate the Private Information that those companies store, the stolen information often ends up on the dark web where malicious actors buy and sell that information for profit.[19]

47. For example, when the U.S. Department of Justice announced their seizure of AlphaBay—the largest online "dark market"—in 2017, AlphaBay had more than 350,000 listings, many of which concerned stolen or fraudulent documents that could be used to assume another person's identity."[20] Marketplaces similar to the now-defunct AlphaBay continue to be "awash with [PII] belonging to victims from countries all over the world."[21]

48. PII remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details

[19] *Shining a Light on the Dark Web with Identity Monitoring*, IDENTITYFORCE (Dec. 28, 2020) https://www.identityforce.com/blog/shining-light-dark-web-identity-monitoring (last visited May 14, 2025).
[20] *Stolen PII & Ramifications: Identity Theft and Fraud on the Dark Web*, ARMOR (April 3, 2018), https://res.armor.com/resources/blog/stolen-pii-ramifications-identity-theft-fraud-dark-web/ (last visited May 14, 2025).
[21] *Id.*

have a price range of $50 to $200.[22] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[23]

49. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses in 2019, resulting in more than $3.5 billion in losses to individuals and business victims.[24]

50. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."[25] Defendant did not rapidly report to Plaintiff and Class Members that their Private Information had been stolen. Defendant has yet to notify impacted people of the Data Breach.

51. As a result of the Data Breach, the Private Information of Plaintiff and Class Members has been exposed to criminals for misuse. The injuries suffered by Plaintiff and Class Members, or likely to be suffered as a direct result of Defendant's Data Breach, include: (a) theft of their Private Information; (b) costs associated with the detection and prevention of identity theft; (c) costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the consequences of this Breach; (d) invasion of privacy; (e) the emotional distress, stress, nuisance, and annoyance of responding to, and resulting from, the Data Breach; (f) the actual and/or imminent injury arising from actual and/or potential fraud and identity theft resulting from their personal data being placed in the hands of the ill-intentioned hackers and/or criminals; (g) damage to and diminution in value of their personal data

---

[22] *Id.*

[23] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015) https://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited May 14, 2025).

[24] *2019 Internet Crime Report Released*, FBI (Feb. 11, 2020) https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120#:~:text=IC3%20received%20467%2C361%20complaints%20in,%2Ddelivery%20scams%2C%20and%20extortion (last visited May 14, 2025).

[25] *Id.*

entrusted to Defendant with the mutual understanding that Defendant would safeguard their Private Information against theft and not allow access to and misuse of their personal data by any unauthorized third party; and (h) the continued risk to their Private Information, which remains in the possession of Defendant, and which is subject to further injurious breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Private Information.

52. In addition to a remedy for economic harm, Plaintiff and Class Members maintain an interest in ensuring that their Private Information is secure, remains secure, and is not subject to further misappropriation and theft.

53. Defendant disregarded the rights of Plaintiff and Class Members by (a) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that its network servers were protected against unauthorized intrusions; (b) failing to disclose that it did not have adequately robust security protocols and training practices in place to safeguard Plaintiff's and Class Members' Private Information; (c) failing to take standard and reasonably available steps to prevent the Data Breach; (d) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (e) failing to provide Plaintiff and Class Members prompt and accurate notice of the Data Breach.

54. The actual and adverse effects to Plaintiff and Class Members, including the imminent, immediate, and continuing increased risk of harm for identity theft, identity fraud and/or medical fraud directly or proximately caused by Defendant's wrongful actions and/or inaction and the resulting Data Breach require Plaintiff and Class Members to take affirmative acts to recover their peace of mind and personal security including, without limitation, purchasing credit reporting services, purchasing credit monitoring and/or internet monitoring services, frequently obtaining,

purchasing and reviewing credit reports, bank statements, and other similar information, instituting and/or removing credit freezes and/or closing or modifying financial accounts, for which there is a financial and temporal cost. Plaintiff and other Class Members have suffered, and will continue to suffer, such damages for the foreseeable future.

F. **Plaintiff Martha Proffitt's Experience**

55. Plaintiff Martha Proffitt is a patient of Defendant.

56. As a condition of receiving medical services from Defendant, Plaintiff was required to supply Defendant with her Private Information—including her name, date of birth, Social Security number, driver's license or state identification number, phone number, and email address.

57. In late April 2025, Defendant sent Plaintiff a text message informing her that it was impacted by a Data Breach.

58. Defendant was in possession of Plaintiff's Private Information before, during and after the Data Breach.

59. Plaintiff reasonably understood and expected that Defendant would safeguard her Private Information and timely and adequately notify her in the event of a data breach. Plaintiff would not have allowed Defendant, or anyone in Defendant's position, to maintain her Private Information if she believed that Defendant would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

60. Plaintiff greatly values her privacy and Private Information and takes reasonable steps to maintain the confidentiality of her Private Information. Plaintiff is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

61. Plaintiff stores any and all documents containing Private Information in a secure location and destroys any documents she receives in the mail that contain any Private Information or that may contain any information that could otherwise be used to compromise her identity and credit card accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

62. As a result of the Data Breach, Plaintiff has spent considerable time researching the Data Breach, reviewing her bank accounts, monitoring her credit report, changing her passwords and other necessary mitigation efforts. This is valuable time that Plaintiff spent at Defendant's direction and that she otherwise would have spent on other activities, including but not limited to work and/or recreation.

63. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress that her Private Information may be misused.

64. Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff will continue to be at present and continued increased risk of identity theft and fraud for years to come.

65. Plaintiff has a continuing interest in ensuring that her Private Information, which upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

66. As a direct and traceable result of the Data Breach, Plaintiff suffered actual injury and damages after her Private Information was compromised and stolen in the Data Breach, including, but not limited to: (a) lost time and money related to monitoring her accounts and credit reports for fraudulent activity; (b) loss of privacy due to her Private Information being accessed and stolen by cybercriminals; (c) loss of the benefit of the bargain because Defendant did not

adequately protect her Private Information; (d) emotional distress because identity thieves now possess her first and last name paired with her Social Security number and other sensitive information; (e) imminent and impending injury arising from the increased risk of fraud and identity theft now that her Private Information has been stolen and likely published on the dark web; (f) diminution in the value of her Private Information, a form of intangible property that Defendant obtained from Plaintiff; and (g) other economic and non-economic harm.

CLASS ALLEGATIONS

67. Plaintiff brings this class action, individually and on behalf of the following Class:

> All persons who were impacted by the Data Breach announced by Defendant in April 2025 (the "Class").

68. Specifically excluded from the Class are Defendant, its officers, directors, agents, trustees, parents, children, corporations, trusts, representatives, principals, servants, partners, joint venturers, or entities controlled by Defendant, and its heirs, successors, assigns, or other persons or entities related to or affiliated with Defendant and/or its officers and/or directors, the judge assigned to this action, and any member of the judge's immediate family.

69. Plaintiff reserves the right to amend the Class definitions above if further investigation and/or discovery reveals that the Class should be expanded, narrowed, divided into subclasses, or otherwise modified in any way.

70. This action may be certified as a class action because it satisfies the numerosity, commonality, typicality, adequacy, and superiority requirements therein.

71. Numerosity: The Class is so numerous that joinder of all Class Members is impracticable. Although the precise number of such persons is unknown, and the facts are presently within the sole knowledge of Defendant, upon information and belief, Plaintiff estimates

that the Class is comprised of thousands of Class Members, if not more. The Class is sufficiently numerous to warrant certification.

72. Typicality of Claims: Plaintiff's claims are typical of those of other Class Members because Plaintiff, like the unnamed Class, had her Private Information compromised as a result of the Data Breach. Plaintiff is a member of the Class, and her claims are typical of the claims of the members of the Class. The harm suffered by Plaintiff is similar to that suffered by all other Class Members which was caused by the same misconduct by Defendant.

73. Adequacy of Representation: Plaintiff will fairly and adequately represent and protect the interests of the Class. Plaintiff has no interests antagonistic to, nor in conflict with, the Class. Plaintiff has retained competent counsel who are experienced in consumer and commercial class action litigation and who will prosecute this action vigorously.

74. Superiority: A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Because the monetary damages suffered by individual Class Members are relatively small, the expense and burden of individual litigation make it impossible for individual Class Members to seek redress for the wrongful conduct asserted herein. If Class treatment of these claims is not available, Defendant will likely continue its wrongful conduct, will unjustly retain improperly obtained revenues, or will otherwise escape liability for its wrongdoing as asserted herein.

75. Predominant Common Questions: The claims of all Class Members present common questions of law or fact, which predominate over any questions affecting only individual Class Members, including:

a. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

b. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

c. Whether Defendant's storage of Plaintiff's and Class Member's Private Information was done in a negligent manner;

d. Whether Defendant had a duty to protect and safeguard Plaintiff's and Class Members' Private Information;

e. Whether Defendant's conduct was negligent;

f. Whether Defendant's conduct violated Plaintiff's and Class Members' privacy;

g. Whether Defendant's conduct violated the statutes as set forth herein;

h. Whether Defendant took sufficient steps to secure individuals' Private Information;

i. Whether Defendant was unjustly enriched; and

j. The nature of relief, including damages and equitable relief, to which Plaintiff and Class Members are entitled.

76. Information concerning Defendant's policies is available from Defendant's records.

77. Plaintiff knows of no difficulty which will be encountered in the management of this litigation which would preclude its maintenance as a class action.

78. The prosecution of separate actions by individual members of the Class would run the risk of inconsistent or varying adjudications and establish incompatible standards of conduct

for Defendant. Prosecution as a class action will eliminate the possibility of repetitious and inefficient litigation.

79. Given that Defendant had not indicated any changes to its conduct or security measures, monetary damages are insufficient and there is no complete and adequate remedy at law.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

80. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above in paragraphs 1 through 18 and paragraphs 23 through 65 as though fully set forth herein.

81. Plaintiff brings this claim individually and on behalf of the Class Members.

82. Defendant knowingly collected, came into possession of, and maintained Plaintiff's and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

83. Defendant had a duty to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiff's and Class Members' Private Information.

84. Defendant had, and continues to have, a duty to timely disclose that Plaintiff's and Class Members' Private Information within its possession was compromised and precisely the types of information that were compromised.

85. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards, applicable standards of care from statutory authority like Section 5 of the FTC Act, and other requirements discussed herein, and to ensure that its

systems and networks, and the personnel responsible for them, adequately protected individuals' Private Information.

86. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its patients. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Plaintiff and Class Members from a data breach.

87. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

88. Defendant breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' Private Information.

89. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiff's and Class Members' Private Information;

b. Failing to adequately monitor the security of its networks and systems; and

c. Failing to periodically ensure that its computer systems and networks had plans in place to maintain reasonable data security safeguards.

90. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' Private Information within Defendant's possession.

91. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiff's and Class Members' Private Information.

92. Defendant, through its actions and/or omissions, unlawfully breached its duty to timely disclose to Plaintiff and Class Members that the Private Information within Defendant's possession might have been compromised and precisely the type of information compromised.

93. Defendant breached the duties set forth in 15 U.S.C. § 45, the FTC guidelines, the National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity, and other industry guidelines. In violation of 15 U.S.C. § 45, Defendant failed to implement proper data security procedures to adequately and reasonably protect Plaintiff's and Class Members' Private Information. In violation of the FTC guidelines, *inter alia,* Defendant did not protect the Private Information it keeps; failed to properly dispose of personal information that was no longer needed; failed to encrypt information stored on computer networks; lacked the requisite understanding of its networks' vulnerabilities; and failed to implement policies to correct security issues.

94. It was foreseeable that Defendant's failure to use reasonable measures to protect Plaintiff's and Class Members' Private Information would result in injury to Plaintiff and Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches.

95. It was foreseeable that the failure to adequately safeguard Plaintiff's and Class Members' Private Information would result in injuries to Plaintiff and Class Members.

96. Defendant's breach of duties owed to Plaintiff and Class Members caused Plaintiff's and Class Members' Private Information to be compromised.

97. But for Defendant's negligent conduct and breach of the above-described duties owed to Plaintiff and Class Members, their Private Information would not have been compromised.

98. As a result of Defendant's failure to timely notify Plaintiff and Class Members that their Private Information had been compromised, Plaintiff and Class Members are unable to take the necessary precautions to mitigate damages by preventing future fraud.

99. As a result of Defendant's negligence and breach of duties, Plaintiff and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes, and Plaintiff and Class Members have and will suffer damages including: a substantial increase in the likelihood of identity theft; the compromise, publication, and theft of their personal information; loss of time and costs associated with the prevention, detection, and recovery from unauthorized use of their personal information; the continued risk to their personal information; future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the personal information compromised as a result of the Data Breach; and overpayment for the services or products that were received without adequate data security.

COUNT II
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Class)

100. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above in paragraphs 1 through 16 and paragraphs 20 through 66 as though fully set forth herein.

101. Section 5 of the FTC Act, 15 U.S.C. 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by Defendant of failing to use reasonable measures to protect Plaintiff's and Class Members' Private Information. Various FTC publications and orders also form the basis of Defendant's duty.

102. Defendant violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect Plaintiff's and Class Members' Private Information and by failing to comply with industry standards.

103. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information obtained and stored and the foreseeable consequences of a data breach on Defendant's systems.

104. Class Members are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes) were intended to protect.

105. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and Class Members.

106. As a result of Defendant's negligence, Plaintiff and Class Members have been harmed and have suffered damages including, but not limited to: damages arising from identity theft and fraud; out-of-pocket expenses associated with procuring identity protection and restoration services; increased risk of future identity theft and fraud, and the costs associated therewith; and time spent monitoring, addressing, and correcting the current and future consequences of the Data Breach.

COUNT III
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

107. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above in paragraphs 1 through 16 and paragraphs 20 through 66 as though fully set forth herein.

108. Plaintiff and Class Members conferred a benefit upon Defendant by providing Defendant with their Private Information.

109. Defendant appreciated or had knowledge of the benefits conferred upon itself by Plaintiff. Defendant also benefited from the receipt of Plaintiff's and Class Members' Private Information.

110. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff's and the Class Members' Private Information because Defendant failed to adequately protect their Private Information. Plaintiff and the proposed Class would not have provided their Private Information to Defendant had they known Defendant would not adequately protect their Private Information.

111. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds received by it because of its misconduct and the Data Breach it caused.

COUNT IV
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class)

112. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above in paragraphs 1 through 16 and paragraphs 20 through 66 as though fully set forth herein.

113. Plaintiff and the Class provided and entrusted their Private Information to Defendant. Plaintiff and the Class provided their Private Information to Defendant as part of a condition of obtaining medical services from Defendant.

114. In so doing, Plaintiff and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had

been breached and compromised or stolen, in return for the business services provided by Defendant. Implied in these exchanges was a promise by Defendant to ensure that the Private Information of Plaintiff and Class Members in its possession was secure.

115. Pursuant to these implied contracts, Plaintiff and Class Members provided Defendant with their Private Information. In exchange, Defendant agreed to, among other things, and Plaintiff and the Class understood that Defendant would: (1) provide medical services to Plaintiff and Class Members'; (2) take reasonable measures to protect the security and confidentiality of Plaintiff and Class Members' Private Information; and (3) protect Plaintiff and Class Members' Private Information in compliance with federal and state laws and regulations and industry standards.

116. Implied in these exchanges was a promise by Defendant to ensure the Private Information of Plaintiff and Class Members in its possession was only used to provide the agreed-upon reasons, and that Defendant would take adequate measures to protect Plaintiff and Class Members' Private Information.

117. A material term of this contract is a covenant by Defendant that it would take reasonable efforts to safeguard that information. Defendant breached this covenant by allowing Plaintiff and Class Members' Private Information to be accessed in the Data Breach.

118. Indeed, implicit in the agreement between Defendant and Plaintiff and Class Members was the obligation that both parties would maintain information confidentially and securely.

119. These exchanges constituted an agreement and meeting of the minds between the parties.

120. When the parties entered into an agreement, mutual assent occurred. Plaintiff and Class Members would not have disclosed their Private Information to Defendant but for the prospect of utilizing Defendant services. Conversely, Defendant presumably would not have taken Plaintiff and Class Members' Private Information if it did not intend to provide Plaintiff and Class Members with its services.

121. Defendant was therefore required to reasonably safeguard and protect the Private Information of Plaintiff and Class Members from unauthorized disclosure and use.

122. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of their implied contracts with Defendant and would have instead retained the opportunity to control their Private Information.

123. Defendant breached the implied contracts with Plaintiff and Class Members by failing to reasonably safeguard and protect Plaintiff and Class Members' Private Information.

124. Defendant's failure to implement adequate measures to protect the Private Information of Plaintiff and Class Members violated the purpose of the agreement between the parties.

125. As a proximate and direct result of Defendant's breaches of its implied contracts with Plaintiff and Class Members, Plaintiff and the Class Members suffered damages as described in detail above.

COUNT V
BREACH OF CONFIDENCE
(On Behalf of Plaintiff and the Class)

126. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above in paragraphs 1 through 16 and paragraphs 20 through 66 as though fully set forth herein.

127. At all times during Plaintiff's and Class Members' interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiff's and Class Members' Private Information that Plaintiff and Class Members entrusted to Defendant.

128. As alleged herein and above, Defendant's relationship with Plaintiff and the Class was governed by terms and expectations that Plaintiff's and the Class Members' Private Information would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

129. Plaintiff and the Class entrusted Defendant with their Private Information with the explicit and implicit understandings that Defendant would protect and not permit the Private Information to be disseminated to any unauthorized third parties.

130. Plaintiff and the Class also entrusted Defendant with their Private Information with the explicit and implicit understandings that Defendant would take precautions to protect that Private Information from unauthorized disclosure.

131. Defendant voluntarily received Plaintiff's and Class Members' Private Information in confidence with the understanding that their Private Information would not be disclosed or disseminated to the public or any unauthorized third parties.

132. As a result of Defendant's failure to prevent and avoid the Data Breach from occurring, Plaintiff's and Class Members' Private Information was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and Class Members' confidence, and without their express permission.

133. As a direct and proximate cause of Defendant's actions and omissions, Plaintiff and the Class have suffered damages.

134. But for Defendant's disclosure of Plaintiff's and Class Members' Private Information in violation of the parties' understanding of confidence, their Private Information would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data Breach was the direct and legal cause of the theft of Plaintiff's and Class Members' Private Information as well as the resulting damages.

135. The injury and harm Plaintiff and the Class suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff's and Class Members' Private Information. Defendant knew or should have known its methods of accepting and securing Plaintiff's and Class Members' Private Information was inadequate as it relates to, at the very least, securing servers and other equipment containing Plaintiff's and Class Members' Private Information.

136. As a direct and proximate result of Defendant's breach of its confidence with Plaintiff and the Class, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) identity theft; (ii) the loss of the opportunity how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual present and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect

the Private Information individuals; and (viii) present and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

137. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and the Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

COUNT VI
MISSOURI MERCHANDISE PRACTICES ACT
Mo. Rev. Stat. §§ 407.010, *et seq.*
(On behalf of Plaintiff and the Class)

138. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above in paragraphs 1 through 16 and paragraphs 20 through 66 as though fully set forth herein.

139. Defendant is a "person" as defined by Mo. Rev. Stat. § 407.010(5).

140. Defendant engaged in "sales" of and "advertisements" for "merchandise" in Missouri and engaged in trade or commerce directly or indirectly affecting the people of Missouri, as defined by Mo. Rev. Stat. § 407.010(1), (4), (6) and (7).

141. Defendant engaged in unlawful, unfair, and deceptive acts and practices, in connection with the sale or advertisement of merchandise in trade or commerce, in violation of Mo. Rev. Stat. § 407.020(1), including:

a. Failing to implement and maintain reasonable security and privacy measures to Plaintiff and Class Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and properly improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Class Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Class Members' Private information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiff and Class Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

142. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' Private Information.

143. Defendant intended to mislead Plaintiff and Class Members and induce them to rely on its misrepresentations and omissions.

144. Defendant acted intentionally, knowingly, and maliciously to violate Missouri's Merchandise Practices Act, and recklessly disregarded Plaintiff and Class Members' rights. Defendant's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

145. As a direct and proximate result of Defendant's unlawful, unfair, and deceptive acts and practices, Plaintiff and Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Private information; overpayment for Defendant's services; loss of the value of access to their Private Information; and the value of identity protection services made necessary by the Data Breach.

146. Plaintiff and Class Members, seek all monetary and non-monetary relief allowed by law, including actual damages, punitive damages, attorneys' fees and costs, injunctive relief, and any other appropriate relief.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, seeks judgment against Defendant, as follows:

(a) For an order determining that this action is properly brought as a class action and certifying Plaintiff as the representative of the Class and her counsel as Class Counsel;

(b) For an order declaring that Defendant's conduct violates the laws referenced herein;

(c) For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

(d) For damages in amounts to be determined by the Court and/or jury;

(e) For an award of statutory damages or penalties to the extent available;

(f) For pre-judgment interest on all amounts awarded;

(g) For an order of restitution and all other forms of monetary relief; and

(h) Such other and further relief as the Court deems necessary and appropriate.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury of all claims in this Class Action Complaint so triable.

Dated: May 14, 2025

Respectfully submitted,

By: */s/ John F. Garvey*

John F. Garvey, #35879 (MO)
Colleen Garvey, #72809 (MO)
Ellen A. Thomas, #73043
STRANCH, JENNINGS & GARVEY, PLLC
701 Market Street, Suite 1510
St. Louis, MO 63101
Tel: (314) 390-6750
jgarvey@stranchlaw.com
cgarvey@stranchlaw.com
ethomas@stranchlaw.com

J. Gerard Stranch, IV (TN BPR #23045)*
Grayson Wells #73068 (MO)
STRANCH, JENNINGS, & GARVEY, PLLC
223 Rosa Parks Ave. Suite 200
Nashville, TN 37203
Telephone: 615/254-8801
gstranch@stranchlaw.com
gwells@stranchlaw.com

Casondra Turner*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN PLLC
800 S. Gay Street, Suite 1100
Knoxville, TN 37929
Telephone: (866) 252-0878
Fax: (771) 772-3086
cturner@milberg.com

Attorneys for Plaintiff and the Proposed Class

- *Pro Hac Vice* forthcoming

IN THE CIRCUIT COURT OF ST. LOUIS COUNTY
STATE OF MISSOURI

MARTHA PROFFITT, individually and on behalf of all others similarly situated, Plaintiff, v. AMERICAN MULTISPECIALTY GROUP, INC. d/b/a ESSE HEALTH, Defendant.	**Case No.: 25SL-CC05304** **Division No. 9** **JURY TRIAL DEMANDED**

MOTION FOR APPOINTMENT OF SPECIAL PROCESS SERVER

Pursuant to Missouri Rules of Civil Procedure, Plaintiff hereby requests the Court appoint H&H Investigations, 4432 Hazelgreen Dr., St. Louis, MO 63119, phone: 314-225-8114, who is not a party to this cause and is not less than 18 years of age, be appointed as Special Process Server to serve all pleadings in this case required by law to be served on Defendant: American Multispecialty Group, Inc., d/b/a Esse Health at 12655 Olive Blvd., Floor 4, St. Louis, MO 63141.

Dated: May 14, 2025

Respectfully submitted,

By: */s/ John F. Garvey*

John F. Garvey, #35879 (MO)
Colleen Garvey, #72809 (MO)
Ellen A. Thomas, #73043
STRANCH, JENNINGS & GARVEY, PLLC
701 Market Street, Suite 1510
St. Louis, MO 63101
Tel: (314) 390-6750
jgarvey@stranchlaw.com
cgarvey@stranchlaw.com
ethomas@stranchlaw.com

J. Gerard Stranch, IV (TN BPR #23045)*
Grayson Wells #73068 (MO)
STRANCH, JENNINGS, & GARVEY, PLLC
223 Rosa Parks Ave. Suite 200
Nashville, TN 37203
Telephone: 615/254-8801
gstranch@stranchlaw.com
gwells@stranchlaw.com

Casondra Turner*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN PLLC
800 S. Gay Street, Suite 1100
Knoxville, TN 37929
Telephone: (866) 252-0878
Fax: (771) 772-3086
cturner@milberg.com

Attorneys for Plaintiff and the Proposed Class

- *Pro Hac Vice* forthcoming

JOAN M. GILMER
CIRCUIT CLERK
ST. LOUIS COUNTY CIRCUIT COURT
105 SOUTH CENTRAL AVENUE
CLAYTON, MISSOURI 63105

IN THE CIRCUIT COURT OF ST. LOUIS COUNTY, MISSOURI

CASE NUMBER: 25SL-CC05304 COURT DATE:
PLAINTIFF: MARTHA PROFFITT COURT TIME:
DEFENDANT: AMERICAN MULTISPECIALTY GROUP, INC., D/B/A ESSE HEALTH, DIVISION:
DATE OF DISMISSAL NOTICE: 19-MAY-2025

DISMISSAL NOTICE

Your petition/pleading(s) have been accepted but no summons or notice can be issued based on the pleadings filed by the party initiating the above referenced case. Corrective pleadings are necessary. The Court cannot proceed further at this time. Please file corrective pleadings as follows:

NO SUMMONS ISSUED DUE TO THE PETITION MISSING THE DEFENDANT'S SERVICE ADDRESS. E-FILE A MEMO INCLUDING THE DEFENDANT'S SERVICE ADDRESS SO THE CASE CAN BE FURTHER PROCESSED. FOR FUTURE REFERENCE, THE DFT'S SERVICE ADDRESS MUST BE LISTED ON THE PETITION UNDER THE DFT'S NAME. ONCE THE CORRECTION IS E-FILED, CONTACT THE CLERK AT 314-615-8470.

The party initiating this case must file pleadings that correct these insufficiencies within seven (7) business days of the date this *Dismissal Notice* is issued or this case will be dismissed for failure to prosecute with costs assessed to initiating party in accordance with Rule 77.01. No extensions will be permitted unless otherwise ordered by the Court.

Please return this memo with the corrected or new pleading.

For additional information regarding this matter you may contact: ADAM at: (314) 615-8470.

JOAN GILMER, CIRCUIT CLERK

IN THE CIRCUIT COURT OF ST. LOUIS COUNTY
STATE OF MISSOURI

MARTHA PROFFITT, individually and on behalf of all others similarly situated, Plaintiff, v. AMERICAN MULTISPECIALTY GROUP, INC. d/b/a ESSE HEALTH, Defendant.	**Case No.: 25SL-CC05304** **Division No. 9** **JURY TRIAL DEMANDED**

MEMORANDUM TO THE CLERK

Plaintiffs by and through their attorneys of record hereby request that the clerk issue a summons for service upon the following Defendant, to be served by special process server:

American Multispecialty Group, Inc., d/b/a Esse Health
12655 Olive Blvd., Floor 4
St. Louis, MO 63141

Dated: May 19, 2025

Respectfully submitted,

By: */s/ John F. Garvey*

John F. Garvey, #35879 (MO)
Colleen Garvey, #72809 (MO)
Ellen A. Thomas, #73043
STRANCH, JENNINGS & GARVEY, PLLC
701 Market Street, Suite 1510
St. Louis, MO 63101
Tel: (314) 390-6750
jgarvey@stranchlaw.com
cgarvey@stranchlaw.com
ethomas@stranchlaw.com

J. Gerard Stranch, IV (TN BPR #23045)*
Grayson Wells #73068 (MO)
STRANCH, JENNINGS, & GARVEY, PLLC
223 Rosa Parks Ave. Suite 200
Nashville, TN 37203
Telephone: 615/254-8801
gstranch@stranchlaw.com
gwells@stranchlaw.com

Casondra Turner*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN PLLC
800 S. Gay Street, Suite 1100
Knoxville, TN 37929
Telephone: (866) 252-0878
Fax: (771) 772-3086
cturner@milberg.com

Attorneys for Plaintiff and the Proposed Class

- *Pro Hac Vice* forthcoming

In the
CIRCUIT COURT
Of St. Louis County, Missouri

For File Stamp Only

Martha Proffitt
Plaintiff/Petitioner

vs.

Ameican Multispecialty Group, Inc.
Defendant/Respondent

May 19, 2025
Date

25SL-CC05304
Case Number

9
Division

REQUEST FOR APPOINTMENT OF PROCESS SERVER

Comes now Plaintiff, pursuant
Requesting Party
to Local Rule 28, and at his/her/its own risk requests the appointment of the Circuit Clerk of

H&H Investigations, 432 Hazelgreen Dr., St. Louis, MO 63119 (314) 225-8114
Name of Process Server — Address — Telephone

Name of Process Server — Address or in the Alternative — Telephone

Name of Process Server — Address or in the Alternative — Telephone

Natural person(s) of lawful age to serve the summons and petition in this cause on the below named parties. This appointment as special process server does not include the authorization to carry a concealed weapon in the performance thereof.

SERVE:
American Multispecialty Group, Inc.
Name
12655 Olive Blvd., Floor 4
Address
St. Louis, MO 63141
City/State/Zip

SERVE:
Name
Address
City/State/Zip

SERVE:
Name
Address
City/State/Zip

SERVE:
Name
Address
City/State/Zip

Appointed as requested:
JOAN M. GILMER, Circuit Clerk

By
Deputy Clerk

Date

Signature of Attorney/Plaintiff/Petitioner
35879
Bar No.
John F. Garvey
Address
(314) 390-6750
Phone No. — Fax No.

CCADM62-WS Rev. 07/22

Local Rule 28. SPECIAL PROCESS SERVERS

(1) Any Judge may appoint a Special Process Server in writing in accordance with the law and at the risk and expense of the requesting party except no special process server shall be appointed to serve a garnishment [except as allowed by Missouri Supreme Court Rule 90.03(a)].

This appointment as Special Process Server does not include the authorization to carry a concealed weapon in the performance thereof.

(2) The Circuit Clerk may appoint a natural person other than the Sheriff to serve process in any cause in accordance with this subsection;

(A) Appointments may list more than one server as alternates.

(B) The appointment of a person other than the Sheriff to serve process shall be made at the risk and expense of the requesting party.

(C) Any person of lawful age, other than the Sheriff, appointed to serve process shall be a natural person and not a corporation or other business association.

(D) No person, other than the Sheriff, shall be appointed to serve any order, writ or other process which requires any levy, seizure, sequestration, garnishment, [except as allowed by Missouri Supreme Court Rule 90.03(a)], or other taking.

(E) Requests for appointment of a person other than the Sheriff to serve process shall be made on a "Request for Appointment of Process Server" electronic form, which may be found on the Court's Web Site, https://stlcountycourts.com/forms/associate-civil/request-process-server/

(F) This appointment as Special Process Server does not include the authorization to carry a concealed weapon in the performance thereof.

SERVICE RETURN

Any service by the St. Louis County Sheriff's Office shall be scanned into the courts case management system. Any service by another Sheriff or a Special Process Server or any other person authorized to serve process shall return to the attorney or party who sought service and the attorney shall file the return electronically to the Circuit Clerk.

Summons in Civil Case

IN THE 21ST JUDICIAL CIRCUIT, ST. LOUIS COUNTY, MISSOURI

Judge or Division: DAVID L VINCENT III	**Case Number: 25SL-CC05304**	
Plaintiff/Petitioner: MARTHA PROFFITT vs.	Plaintiff's/Petitioner's Attorney/Address JOHN FRANCIS GARVEY JR 701 MARKET ST SUITE 1510 ST LOUIS, MO 63101	
Defendant/Respondent: AMERICAN MULTISPECIALTY GROUP, INC. DBA: ESSE HEALTH	Court Address: ST LOUIS COUNTY COURT BUILDING 105 SOUTH CENTRAL AVENUE CLAYTON, MO 63105	
Nature of Suit: CC Breach of Contract		(Date File Stamp for Return)

The State of Missouri to: AMERICAN MULTISPECIALTY GROUP, INC.
Alias:
DBA: ESSE HEALTH

C/O DAVID KEARNEY
12655 OLIVE BLVD., FLOOR 4
ST. LOUIS, MO 63141

You are summoned to appear before this court and to file your pleading to the petition, a copy of which is attached, and to serve a copy of your pleading upon the attorney for plaintiff/petitioner at the above address all within 30 days after receiving this summons, exclusive of the day of service. If you fail to file your pleading, judgment by default may be taken against you for the relief demanded in the petition.

COURT SEAL OF

ST. LOUIS COUNTY

19-MAY-2025
Date

/S/ Adam Dockery
Clerk

Further Information:
AD

Officer's or Server's Return

Note to serving officer: Service should be returned to the court within 30 days after the date of issue.

I certify that I have served the above Summons by: (check one)

☐ delivering a copy of the summons and petition to the defendant/respondent.

☐ leaving a copy of the summons and petition at the dwelling house or usual place of abode of the defendant/respondent with _____, a person at least 18 years of age residing therein.

☐ (for service on a corporation) delivering a copy of the summons and petition to:
_____ (name) _____ (title).

☐ other: _____.

Served at _____ (address)
in _____ (County/City of St. Louis), MO, on _____ (date)
at _____ (time).

_____ _____
Printed Name of Officer or Server Signature of Officer or Server

Must be sworn before a notary public if not served by an authorized officer.
Subscribed and sworn to before me on _____ (date).

(Seal)

My commission expires: _____ _____
Date Notary Public

Service Fees (if applicable)

Summons	$_____
Non Est	$_____
Sheriff's Deputy Salary	
Supplemental Surcharge	$ 10.00
Mileage	$_____ (_____ miles @ $._____ per mile)
Total	**$_____**

A copy of the summons and petition must be served on **each** defendant/respondent. For methods of service on all classes of suits, see Supreme Court Rule 54.

THE CIRCUIT COURT OF ST. LOUIS COUNTY, MISSOURI

Twenty First Judicial Circuit

NOTICE OF ALTERNATIVE DISPUTE RESOLUTION SERVICES

Purpose of Notice

As a party to a lawsuit in this court, you have the right to have a judge or jury decide your case. However, most lawsuits are settled by the parties before a trial takes place. This is often true even when the parties initially believe that settlement is not possible. A settlement reduces the expense and inconvenience of litigation. It also eliminates any uncertainty about the results of a trial.

Alternative dispute resolution services and procedures are available that may help the parties settle their lawsuit faster and at less cost. Often such services are most effective in reducing costs if used early in the course of a lawsuit. Your attorney can aid you in deciding whether and when such services would be helpful in your case.

Your Rights and Obligations in Court Are Not Affected By This Notice

You may decide to use an alternative dispute resolution procedure if the other parties to your case agree to do so. In some circumstances, a judge of this court may refer your case to an alternative dispute resolution procedure described below. These procedures are not a substitute for the services of a lawyer and consultation with a lawyer is recommended. Because you are a party to a lawsuit, you have obligations and deadlines which must be followed whether you use an alternative dispute resolution procedure or not. **IF YOU HAVE BEEN SERVED WITH A PETITION, YOU MUST FILE A RESPONSE ON TIME TO AVOID THE RISK OF DEFAULT JUDGMENT, WHETHER OR NOT YOU CHOOSE TO PURSUE AN ALTERNATIVE DISPUTE RESOLUTION PROCEDURE.**

Alternative Dispute Resolution Procedures

There are several procedures designed to help parties settle lawsuits. Most of these procedures involve the services of a neutral third party, often referred to as the “neutral,” who is trained in dispute resolution and is not partial to any party. The services are provided by individuals and organizations who may charge a fee for this help. Some of the recognized alternative dispute resolutions procedures are:

(1) Advisory Arbitration: A procedure in which a neutral person or persons (typically one person or a panel of three persons) hears both sides and decides the case. The arbitrator’s decision is not binding and simply serves to guide the parties in trying to settle their lawsuit. An arbitration is typically less formal than a trial, is usually shorter, and may be conducted in a private setting at a time mutually agreeable to the parties. The parties, by agreement, may select the arbitrator(s) and determine the rules under which the arbitration will be conducted.

(2) Mediation: A process in which a neutral third party facilitates communication between the parties to promote settlement. An effective mediator may offer solutions that have not been considered by the parties or their lawyers. A mediator may not impose his or her own judgment on the issues for that of the parties.

(3) Early Neutral Evaluation ("ENE"): A process designed to bring the parties to the litigation and their counsel together in the early pretrial period to present case summaries before and receive a non-binding assessment from an experienced neutral evaluator. The objective is to promote early and meaningful communication concerning disputes, enabling parties to plan their cases effectively and assess realistically the relative strengths and weaknesses of their positions. While this confidential environment provides an opportunity to negotiate a resolution, immediate settlement is not the primary purpose of this process.

(4) Mini-Trial: A process in which each party and their counsel present their case before a selected representative for each party and a neutral third party, to define the issues and develop a basis for realistic settlement negotiations. The neutral third party may issue an advisory opinion regarding the merits of the case. The advisory opinion is not binding.

(5) Summary Jury Trial: A summary jury trial is a non binding, informal settlement process in which jurors hear abbreviated case presentations. A judge or neutral presides over the hearing, but there are no witnesses and the rules of evidence are relaxed. After the "trial", the jurors retire to deliberate and then deliver an advisory verdict. The verdict then becomes the starting point for settlement negotiations among the parties.

Selecting an Alternative Dispute Resolution Procedure and a Neutral

If the parties agree to use an alternative dispute resolution procedure, they must decide what type of procedure to use and the identity of the neutral. As a public service, the St. Louis County Circuit Clerk maintains a list of persons who are available to serve as neutrals. The list contains the names of individuals who have met qualifications established by the Missouri Supreme Court and have asked to be on the list. The Circuit Clerk also has Neutral Qualifications Forms on file. These forms have been submitted by the neutrals on the list and provide information on their background and expertise. They also indicate the types of alternative dispute resolution services each neutral provides.

A copy of the list may be obtained by request in person and in writing to: Circuit Clerk, Office of Dispute Resolution Services, 105 South Central Avenue, 5th Floor, Clayton, Missouri 63105. The Neutral Qualifications Forms will also be made available for inspection upon request to the Circuit Clerk.

The List and Neutral Qualification Forms are provided only as a convenience to the parties in selecting a neutral. The court cannot advise you on legal matters and can only provide you with the List and Forms. You should ask your lawyer for further information.

OFFICE OF THE CIRCUIT CLERK
Missouri's 21st Judicial Circuit, St. Louis County
Civil Department
105 South Central Avenue, Clayton, MO 63105
Hours: Monday through Friday 8:00 A.M. to 5:00 P.M.
Phone: 314-615-8029

SPECIAL NEEDS: If you have special needs addressed by the Americans With Disabilities Act. Please notify the Office of the Circuit Clerk at 314-615-8029. FAX 314-615-8739, email at SLCADA@courts.mo.gov, or through Relay Missouri by dialing 711 0r 800-735-2966, at least three business days in advance of the court proceeding.

Summons in Civil Case

IN THE 21ST JUDICIAL CIRCUIT, ST. LOUIS COUNTY, MISSOURI

Judge or Division: DAVID L VINCENT III	**Case Number: 25SL-CC05304**
Plaintiff/Petitioner: MARTHA PROFFITT vs.	Plaintiff's/Petitioner's Attorney/Address JOHN FRANCIS GARVEY JR 701 MARKET ST SUITE 1510 ST LOUIS, MO 63101
Defendant/Respondent: AMERICAN MULTISPECIALTY GROUP, INC. DBA: ESSE HEALTH	Court Address: ST LOUIS COUNTY COURT BUILDING 105 SOUTH CENTRAL AVENUE CLAYTON, MO 63105
Nature of Suit: CC Breach of Contract	(Date File Stamp for Return)

The State of Missouri to: AMERICAN MULTISPECIALTY GROUP, INC.
Alias:
DBA: ESSE HEALTH

C/O DAVID KEARNEY
12655 OLIVE BLVD., FLOOR 4
ST. LOUIS, MO 63141

You are summoned to appear before this court and to file your pleading to the petition, a copy of which is attached, and to serve a copy of your pleading upon the attorney for plaintiff/petitioner at the above address all within 30 days after receiving this summons, exclusive of the day of service. If you fail to file your pleading, judgment by default may be taken against you for the relief demanded in the petition.

COURT SEAL OF

ST. LOUIS COUNTY

19-MAY-2025
Date

/S/ Adam Dockery
Clerk

Further Information:
AD

Case Number: 25SL-CC05304

Officer's or Server's Return

Note to serving officer: Service should be returned to the court within 30 days after the date of issue.

I certify that I have served the above Summons by: (check one)

☐ delivering a copy of the summons and petition to the defendant/respondent.

☐ leaving a copy of the summons and petition at the dwelling house or usual place of abode of the defendant/respondent with _____, a person at least 18 years of age residing therein.

☒ (for service on a corporation) delivering a copy of the summons and petition to:
Robert Richman (name) CFO (title).

☐ other: _____.

Served at 12655 Olive Blvd St. Louis, MO 63141 (address)
in St. Louis (County/City of St. Louis), MO, on 5/20/25 (date)
at 1:52 pm (time).

Joseph Dolan Special Process Server #722 SPS #722
Printed Name of Officer or Server Signature of Officer or Server

Must be sworn before a notary public if not served by an authorized officer.
Subscribed and sworn to before me on 5/21/25 (date).

(Seal)
Diane L McKay
Notary Public, Notary Seal
State of Missouri
St. Louis County
My Commission Expires 4/11/2029
Commission # 13470566

My commission expires: 4/11/29
Date

Notary Public

Service Fees (if applicable)

Summons	$_____
Non Est	$_____
Sheriff's Deputy Salary	
Supplemental Surcharge	$ 10.00
Mileage	$_____ (_____ miles @ $._____ per mile)
Total	$_____

A copy of the summons and petition must be served on **each** defendant/respondent. For methods of service on all classes of suits, see Supreme Court Rule 54.